Security Standards for Electric Market Participants

PURPOSE

Wholesale electric grid operations are highly interdependent, and a failure of one part of the generation, transmission or grid management system can compromise the reliable operation of a major portion of the regional grid. Similarly, the wholesale electric market – as a network of economic transactions and interdependencies – relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch and market software and systems. Because of this mutual vulnerability and interdependence, it is necessary to safeguard the electric grid and market resources and systems by establishing minimum standards for all market participants, to assure that a lack of security for one resource does not compromise security and risk grid and market failure for the market or grid as a whole.

The purpose of these standards is to ensure that electric market participants have a basic Security Program protecting the electric grid and market from the impacts of acts, either accidental or malicious, that aren't authentic or could cause wide-ranging, harmful impacts on grid operations and market resources. A basic Security Program for electric grid and market resources (hereafter referred to as market resources) shall cover governance, planning, prevention, operations, incident response, and business continuity.

Security standards for market resources will primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact the grid or market, and personnel (hereafter the word cyber shall refer to all of these

aspects). In addition, physical security will be addressed to the extent that it is necessary to assure a secure physical environment for cyber resources.

This initial set of security standards represent a minimum set of measures derived from commonly accepted industry standards and practices, such as the Common Criteria, CTSEC, ITSEC, IPSEC, ISO 17799, NIST Guidelines, and the NERC Security Guidelines. Market participants are encouraged to review their individual situation and tolerance for risk and implement a Security Program that goes beyond these basic security standards herein.

APPLICATION

These standards are intended to ensure that appropriate mitigating plans and actions are in place, recognizing the role of the participant in the marketplace and the risks being managed. For the purpose of these security standards, participants are defined as, and the standards shall apply to:

- The market operations of RTO's and ISO's, and their market connections to Control Areas,
- Marketers,
- Transmission Owners,
- Power Producers,
- Load serving entities and other power purchasers,
- NERC and the Reliability Authorities, and
- Tagging (or other similar dispatching) Organizations.

Further, if a power-generating unit participates directly in the grid (i.e. it is electronically dispatched by control centers), the plant control system shall comply with these security

standards. If a power-generating unit participates directly in the electric market (i.e. submits Tagging requests), its market systems shall also comply with these security standards.

COMPLIANCE

These security standards shall become effective on January 1, 2004. Beginning 2004, on January 1 of each year, every participant shall file with FERC a self-certification signed by an officer of the company indicating compliance with these standards and identifying any areas of non-compliance. Failure to comply with these security standards will result in loss of direct access privileges to the electric market.

Malicious acts directed against the electric market, shall be prosecuted by FERC and law enforcement agencies to the full extent of the law, including the recovery of damages.

SECURITY STANDARDS

Governance:

Participant senior management shall designate a management official to be responsible for establishing and managing a basic Security Program for electric market functions and resources.

Security Scope:

Participants shall define their security perimeter, identify the boundaries and defenses for physical and cyber security that delineate and protect the critical resources under their control. The security perimeter shall identify all entry and exit points and the requirements for access controls. A Security Program and policy based on, and implementing these security standards shall be developed to protect critical electric grid and market functions and resources within the security perimeter and at entry and exit points where personnel, supplies or communications may

come and go. Additionally, related procedures shall be created that guide implementation and enforcement of the security standards. Policy and procedures shall be reviewed for appropriateness (due to changes in personnel, technology, equipment configuration, vulnerabilities and threats) as necessary, and at least annually.

Asset Classification and Control:

Electric market assets within the security perimeter shall be classified as to their criticality in maintaining and protecting electric market functions. A classification system shall further define appropriate levels of protection for each level of criticality, and access rights that will be granted for each level of criticality. All critical assets within the perimeter (computers, networks, doorways, etc.) shall have a custodian who ensures that those assets are handled in accordance with their assigned classification scheme.

Personnel:

Any personnel who are authorized access within the security perimeter, or are authorized access to administer, operate or maintain assets within the security perimeter shall be trained on the Security Program and security standards related to their respective positions. This training shall start upon employment, be repeated annually and at career points where significant responsibilities change. Security awareness training shall be provided to all staff.

To the extent permitted by law, personnel required to administer or operate assets classified as critical (according to the participant's classification system) shall undergo background investigation conducted prior to employment, upon promotion to such positions (if not a new hire), and at periodic intervals (not to exceed five years). The participant shall review the results of the background checks and take appropriate action. Individuals shall be disqualified from

administering, operating or accessing critical assets if the individual meets any disqualifying criteria specified by the Federal Bureau of Investigation, Office of Homeland Security, RCMP, or other federal agency.

Access Control:

A process such as transaction logs shall be in place to identify individual users of critical systems and their time of access. Procedures for critical electric grid and market resources within the security perimeter shall be developed that establish and monitor controls for:

1) The assignment of both logical and physical access rights (as defined in the classification system);
2) The prompt disabling of access rights when positions are terminated or job responsibilities no longer require access; and
3) The annual re-evaluation of assigned access rights.

Such authorized personnel -- including visitors and service vendors -- shall only have access (whether logical or physical) to electric market resources within the security perimeter that they are authorized for. Any and all unauthorized personnel allowed temporary access within the security perimeter shall be escorted at all times.

Systems Management:

Procedures for critical electric market resources within the security perimeter shall be developed to monitor and control cyber assets, such as:

- Computers,
- Software,
- Data,
- Servers,

- Routers,
- Modems, and
- Communications channels, whether owned or leased.

At a minimum, these procedures shall address:

1) The use of effective password routines that periodically require changing of passwords, including the replacement of default passwords on newly installed equipment;
2) Authorization and re-validation of computer accounts;
3) Disabling of unauthorized (invalidated, expired) or unused computer accounts;
4) Disabling of unused network services and ports;
5) Secure dial-up modem connections;
6) Firewall software (for routed Internet access);
7) Intrusion Detection Systems (for networked routers and firewalls);
8) Host based intrusion or system failure detection for critical systems;
9) Patch management;
10) Installation and update of anti-virus software checkers.

For critical electric systems, operator logs and Intrusion Detection System logs shall be maintained for the purpose of checking system anomalies and for evidence of suspected unauthorized activity. Appropriate procedures for securing control systems that are critical to the grid or market shall be developed and employed. The procedures shall address:

1) Remote access including modems and other means;
2) Security patch management, as appropriate;
3) Assurance that communication channels are adequate so as not to impact the performance of the control system and its critical functions; and

4) Assurance that system procedures do not impact the performance of the control system and its critical functions.

Procedures for critical electric resources within the security perimeter shall be established to monitor and control physical features, such as:

- Doors,
- Windows,
- Floor space,
- Environmental systems,
- Backup power systems – whether owned or leased.

At a minimum, these procedures shall address:

1) Appropriate security barriers and entry controls; 2)
2) Mechanical and electronic key and badge programs; 3)
3) Access locking of unattended assets; and, 4)
4) Protection from environmental threats and hazards (e.g., loss of cooling).

Critical electric facilities shall restrict the distribution of maps, floor plans and equipment layouts pertaining to those facilities, and restrict the use of signage indicating critical facility locations.

Planning:

Security requirements for critical electric systems within the security perimeter shall be identified, documented and agreed upon prior to development, procurement, enhancement to, installation of and acceptance testing for cyber resources or related physical features. For critical control systems, this means developing cyber security procedures to augment existing test and/or acceptance procedures.

Development and testing of critical electric market systems shall be conducted in system environments that are not interconnected with operational system environments.

Incident Response:

Organizations with critical electric market resources shall have incident response procedures, which define roles, responsibilities and actions to rapidly detect and protect electric resources in the event of harmful or unusual incidents, whether accidental or malicious.

Organizations with critical electric market resources shall report incidents to the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC) and use reporting criteria, thresholds and procedures contained in NERC's Indications, Analysis and Warning (IAW) Program.

Business Continuity:

Every participant operating a critical electric resource shall have contingency plans that define roles, responsibilities and actions for protecting the rest of the electric grid and market from the failure of its own critical resources. Those plans should further define the roles, responsibilities and actions needed to quickly recover or reestablish electric grid and market functions, processes and systems, in the event that a critical physical or cyber resource fails or suffers harm or attack. Such plans shall be tested or exercised regularly.

REFERENCES

The North American Electric Reliability Council (NERC) has established and maintains Security Guidelines for the Electricity Sector. NERC also provides a list of additional sources for security

best practices. These references shall be helpful in developing organization specific security standards and procedures for critical market resources.

ADDENDUM

Annual Self-Certification of Compliance with FERC Security Standards
(Due January 31, 2004, and every January 31st thereafter)

Date: _____

Subject: FERC Filing, Annual Self-Certification re: FERC Security Standards

From: _____(organization name)

_____(organization address)

_____(organization address)

_____(organization address)

This organization certifies the following items regarding FERC security standards for grid-market systems, as of this date:

Compliant	Non-Compliant	
?	?	Management assignment of grid-market system security.
?	?	Security Perimeter defined and documented.
?	?	Security Program and Policy developed and documented.
?	?	Policy, standards, and procedures reviewed at least annually.
?	?	An Asset Classification system defined and implemented.
?	?	Security training requirements for personnel with access to critical assets have been met.
?	?	All personnel receive security awareness training at least annually.
?	?	Critical asset administrators and operators have had background screening within last five years.
?	?	Access control procedures for authorized personnel are implemented.
?	?	Unauthorized personnel inside security perimeter are escorted at all times.
?	?	Cyber procedures for system security have been developed and implementation monitored for compliance.
?	?	Physical procedures for system security have been developed and implementation monitored for compliance.
?	?	Security requirements for developing and testing critical systems have been documented.
?	?	Software development systems are not interconnected with operational systems.
?	?	Incident response plans are implemented.
?	?	ES-ISAC reporting and alert notification procedures are implemented.
?	?	Business continuity plans are established and exercised.

Explanation for Non-Compliant Items:

Name: _____(print)

_____(title)

_____(signature)